IDENTIFICATION SYSTEM FOR AUTHENTICATING BOTH IC CARD AND TERMINAL

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to an identification system for identifying the identities between an IC card issued such as a cash card or credit card and an IC card terminal when the IC card is loaded in the IC card terminal installed in a shop or the like.

2. Description of the Prior Art

Recently, there have been a variety of cards issued by credit card firms or the like, with which commercial commodities can be purchased. As such cards, plastic cards, embossing cards, cards having magnetic stripes, etc. are used. Such cards can be easily forged for illegal use. To prevent this problem, there has recently been developed an information card or so-called IC card, in which an IC module with a personal identification number (PIN) or the like stored therein is embedded in a thin card so that the PIN cannot be readily read out from the outside. This IC card can be difficult to forge and has excellent security. Further, it can store large quantities of information. When the IC card is used for a commercial transaction, it is loaded in an IC card terminal installed at a bank, a shop, etc., and the PIN and other data are input for the identification of the card and cardholder before a predetermined processing is executed.

However, in the IC card system utilizing the IC card and IC card terminal, the PIN data of the cardholder is input from a keyboard of the card terminal in the shop. Therefore, the PIN data input operation is liable to be watched surreptitiously by, for instance, staff members, or other customers in the shop. Also, it is possible that the input PIN data can be read out surreptitiously by providing some surreptitious use of the card terminal itself. Therefore, the IC card has potential security problems during actual transactions. The surreptitious observation of the PIN data input operation can be avoided if care is taken by the person who inputs the secret data. However, if means for surreptitiously reading out data is provided in the card terminal itself, there is no effective countermeasure by the cardholder. Further, when the IC card is forged, there is no countermeasure at all within the card terminal. Therefore, when an IC card is loaded in an IC card terminal, it is necessary to confirm the validity of both the card and the IC card terminal before the PIN data input operation, i.e., in an initial state after loading of or electric communicating with the IC card.

SUMMARY OF THE INVENTION

The invention has been accomplished in view of the above conventional drawbacks, and has therefore an object of providing an identification system, which can avoid illegal card transactions due to forging of an IC card, tampering with an IC card terminal, or using a counterfeit terminal.

The object and other features of the invention can be achieved by providing an identification system comprising:

IC card means;

IC card terminal means capable of electrically communicating with the IC card means when the IC card means is loaded thereon;

said IC card means including first memory means for storing at least data unique to said IC card means and encrypted unique data obtained by encrypting said unique data;

said IC card terminal means including decrypting means for decrypting said encrypted unique data stored in said first memory means to derive decrypted unique data;

said IC card means further including first comparing means for comparing said unique data stored in said first memory means with said decrypted unique data sent from said IC card terminal means so as to judge whether said unique data is coincident with said decrypted unique data; and

said IC card terminal further including second comparing means for comparing said unique data stored in said first memory means and sent from said IC card means with said decrypted unique data so as to judge whether said unique data is coincident with said decrypted unique data, thereby confirming identities of both said IC card means and said IC card terminal means.

BRIEF DESCRIPTION OF THE DRAWINGS

For a better understanding of the above object and the features of the present invention, reference is made to the following detailed description of the invention to be read in conjunction with the accompanying drawings, in which:

FIG. **1** is a perspective view showing an IC card and an IC card terminal used in the identification system according to an embodiment of the invention;

FIG. **2** is a block diagram showing the circuitry of the IC card shown in FIG. **1**;

FIG. **3** is a schematic block diagram showing the circuitry of the IC card terminal shown in FIG. **1**; and

FIG. **4** is a flow chart illustrating an operation of confirming the authenticity of the IC card and IC card terminal in the IC card system.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

An embodiment of this invention will now be described with reference to the accompanying drawings.

IC CARD AND CARD TERMINAL

FIG. **1** shows a perspective view of IC card **11** and IC card terminal (external unit) **12** in an IC card system **100** according to the invention. The IC card terminal **12** has keyboard **13**, display **14** and card inlet **15** for permitting electric connection of terminal **12** to connector section **11***a* of IC card **11**. These terminal parts are provided on top of a terminal housing. Card inlet **15** is provided in a card inlet panel, which is provided with eject push-button **16** for taking out the IC card.

CIRCUIT ARRANGEMENT OF IC CARD

FIG. **2** shows the circuit arrangement of IC card **11** illustrated in FIG. **1**. A data bus line **21** is connected to system controller **22** and system program ROM **23**.

Data RAM **24** and data latch unit **25** are connected to data bus line **21**, and also data memory **28** are connected to data bus line **21** via parallel-connected write controller **26** and read controller **27**. System controller **22** supplies control commands to these circuit elements.